Legal Environments for Digital Trust

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 3 (2012)

Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability

Yianna Danidou
American College, Computer Science Department,
2&3 Omirou Avenue, P.O. Box 22425, 1521 Nicosia, Cyprus
yianna.danidou@ac.ac.cy

Burkhard Schafer
University of Edinburgh,
SCRIPT, School of Law,
Old College Edinburgh, EH8 9YL, UK,
B.Schafer@ed.ac.uk

Abstract. *Trusted Computing and Trustmarks are two approaches developed to enhance internet security and trust and we claim that they are structurally similar and an exercise in mutual learning would be of great benefit for both. We argue that TC philosophy could possibly supplement TMOs so that TMs become to TMOs more than just a mere link while we address critical questions regarding reliance liability. With our present study we propose that the model for adequate TMO liability could possibly be an example of how to deal with the issue of TC's reliance liability.*

.

1. Introduction

This paper argues that Trusted Computing (TC) and Trustmarks (TM) share more than a highly polysemantic word in their names, and that while the respective communities interested in the development and legal regulation of these two approaches to internet security, have in the past seldom attempted to systematically exchange concepts and ideas. Such an exercise in mutual learning is of great potential benefit. In particular, we argue that the more mature debate on the legal implications of TMs is of high relevance for the development and regulation of trusted computing, while conversely the technologically more ambitious TC approach can provide important insights into the user requirements for the next generation of TMs.

As more and more of our activities are carried out online, it has become increasingly clear over the past decades that the Internet, which was never intended for this type and scale of commercial activity, is vulnerable to attacks and criminal activities. Given the widespread acceptance of the commercialization of the Internet, e-commerce has experienced astonishing growth since its development in the 1990's. Security and privacy – amongst other issues[1] – seem to be at the top of consumer's concerns while conducting onli1ne transactions. As recent statistics show, e-consumers do not feel secure at all in the online environment and this has an impact on their willingness to provide personal or payment details over the Internet[2].

[1] CHEN CHENG-HAO & MASOUD SAEEDI, *Building a Trust Model in the Online Market Place*, 5 Journal of Internet Commerce (2006);ASSAFA ENDESHAW, *The Legal Significance of Trustmarks*, 10 Information & Communications Technology Law (2001).
[2] Scoping Study for the Measurement of Trust in the Online Environment. No. DSTI/ICCP/IIS(2005)1/FINAL(2005);Measuring Security and Trust in the Online Environment: A View Using Official Data. No. DSTI/ICCP/IIS(2007)4/FINAL(2008).

We can, broadly speaking, distinguish two risk scenarios: In the first, a consumer gives financial or personal details to a fraudulent website that then abuses the information. In the second, the consumer gives his details to a legitimate e-commerce provider, whose site is then however attacked and compromised by a third party, which steals the information. In the second type of scenario, legitimate users too can become unwittingly helpers of criminal activity when letting their computer become compromised – possibly through a transaction on a fraudulent website as in scenario 1.

To reap the benefits of the ICT revolution, users must be able to trust their system. When asked to pay for goods bought online, to make a bank transfer from an online account, or to apply for a passport at a government run website, it is essential that the user can trust the communication to be secure, and that the party he is communicating with, is the party it claims to be.

This paper uses the notion from the field of trusted systems, according to Shirey's internet security glossary[3] and not the sociological concept[4]. It is used in this latter way in many papers that address similar contexts as ours[5] and benefits from the high level of abstractness that allows it to be applied to both humans and machines. Thus, Trusted systems are systems that can be relied upon to perform certain security policies in an expected manner and in the sense of behavioral consistency: TC "refers to a computer system for which an entity has some level of assurance that (part or all of) the computer system is behaving as expected"[6] for a particular purpose. The outcome ultimately would be to allow the user to 'blindly trust' his computer again, without a constant need for self-monitoring.

This paper aims to show that the similarities between TC and TM are so strong that we can transfer ideas and experiences between these two fields. In particular TC can learn from the discussion of legal problems with TM, including in-build arbitration, while TM can benefit from the TC experience with remote attestation.

2. Trustmarks in a nutshell

Fortunately, the European Union has trust in e-commerce amongst the top places in its digital agenda[7]. The European Commission created a dedicated agency[8] exclusively for achieving high and effective level of network and information security. According to the agenda, the EU takes coordinated measures on network and information security in order to increase trust and confidence in cyberspace.

In an effort to attract and keep consumers, e-businesses seek ways to enhance consumer trust on the Internet to allow this "new way of transferring ownership or right to use good or services through trustmarks.

Trustmarks (TMs) have been developed in the late 1990s as an attempt to develop and gain consumer trust through web signals. The Trustmark Organisations (TMOs) which are in fact Trusted Third Parties (TTPs), are independent parties that provide TMs to online merchants (e-merchants), as a way to label that a product, process or service that the e-merchant offers conforms to specific quality characteristics concerning legitimacy, security

[3] R. SHIREY, RFC2828: Internet Security Glossary (RFC Editor. 2000).
[4] FRANCIS FUKUYAMA, Trust: The Social Virtues and The Creation of Prosperity (Simon & Schuster Free Press Paperbacks book 1st ed. 1995).
[5] BORIS BALACHEFF, et al., *Computing Platform Security in Cyberspace*, 5 Inf. Secur. Tech. Rep. (2000);CHRIS J. MITCHELL, *What is Trusted Computing?, in* Trusted Computing (Chris J. Mitchell ed. 2008).
[6] MITCHELL.
[7] EUROPEAN COMMISSION, 2011/C 54/17 Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe' COM(2010) 245 final § 54 (Office for Official Publication of the EEC ed., Luxembourg, Office for Official Publication of the EEC 2011).
[8] Information security awareness initiatives: Current practice and the measurement of success. pt. 24 (2007).

of transactions, privacy and integrity. TMs thus aim to promote the feeling of security and trust of e-consumers[9] thus influencing them to engage in e-commerce[10] so that when the e-merchant displays the TM on his website, the e-consumers will face only minimal transaction costs (in terms of time invested) to check the integrity of that e-merchant in relation to security, privacy and business practice. This is mostly because e-consumers rely on the reputation of TMOs[11] and on the perception that "a third party gives a written assurance that a product, process, or service conforms to specific characteristics"[12], with other words they consider TMs a form of guarantee[13]. Some TMs offer mechanisms relating to consumer redress [14] i.e. to resolve disputes between the certified e-business and the e-consumer. "Such features vary from assistance in filing the case with a consumer redress mechanism to providing a complete alternative dispute resolution system"[15]

Very briefly, the procedure of giving a TM to an e-merchant follows this pattern: the e-merchant cooperates with the TMOs and asks for a TM, which he gains when he submits a satisfactory self-assessment report referring to the business's security, privacy and practices[16]. Different TMs then vary in the degree of scrutiny of this self assessment, renewal of application and procedures to withdraw it, again should standards slip. However, it is significant to note that a large gap is identified between the online consumers' actual needs for assurance and the assurance that seals are supposed to offer[17].

As computer systems changed in nature and became more and more ubiquitous, many technical challenges arose that cumulated in the realization that system designers must treat trust and trustworthiness as a need-to-have design feature, much more prominently than in the currently implemented ones. Prevention of denial of service, access control against malicious outsiders and insiders and monitoring, and the achievement of scalability are just some of the numerous technical challenges that need to be overcome by current distributed systems. The need for such a platform becomes more imperative by the recognition that it is insufficient to rely on users taking the necessary precautions to protect their systems themselves (by frequently updating firewalls and anti-virus systems) and that the threats and attacks have increased exponentially due to automated attack tools, proliferation of vulnerabilities and increased mobility of users[18]. Instructive in this respect is the CERT Coordination Center and its reports on the extremely large amount of vulnerabilities catalogued until 2008[19].

In addition to the increasing security threats, the easiness to write and spread malicious code (even ubiquitously), the vast number of personal computers along with the substantial use and incredible evolution of the Internet during the last 15 years[20] have led to the conclusion that systems with increased security, high

---

[9] RICHARD W. HOUSTON & GARY K. TAYLOR, *Consumer Perceptions of CPA WebTrustSMAssurances: Evidence of an Expectation Gap*, 3 International Journal of Auditing (1999);JONATHAN W. PALMER, et al., *The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements*, 5 Journal of Computer-Mediated Communication (2000).

[10] STACY E. KOVAR, et al., *Consumer Responses to the CPA WEBTRUST Assurance*, 14 Journal of Information Systems (2000);ELAINE MAULDIN & VAIRAM ARUNACHALAM, *An Experimental Examination of Alternative Forms of Web Assurance for Business-to-Consumer e-Commerce*, 16 Journal of Information Systems (2002).

[11] P. BALBONI, Trustmarks: Third-party liability of trustmark organisations in Europe (2008)

[12] ANDREW RAE, et al., Software Evaluation for Certification (McGraw-Hill, Inc. . 1994).

[13] DWANE HAL DEAN & ABHIJIT BISWAS, *Third-Party Organization Endorsement of Products: An Advertising Cue Affecting Consumer Prepurchase Evaluation of Goods and Services*, 30 Journal of Advertising (2001);CARL PACINI & DAVID SINASON, *Auditor Liability for Electronic Commerce Transaction Assurance: The CPA/CA Webtrust*, 36 American Business Law Journal (1999).

[14] CARLETON S. FIORINA, et al., Consumer Confidence Trustmarks (2001);JAN TRZASKOWSKI, Chapter 3 Legislation and requirements concerning Trustmarks (1.0 ed. 2010).

[15] TRZASKOWSKI.

[16] ENDESHAW.

[17] X. R. HU, et al., *The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective*, 48 DECISION SUPPORT SYSTEMS (2010);MARCUS D. ODOM, et al., *Web Assurance Seals: How and Why They Influence Consumers' Decisions*, 16 Journal of Information Systems (2002).

[18] BRIAN BERGER, *Trusted computing group history*, 10 Inf. Secur. Tech. Rep. (2005).

[19] CERT, *CERT Statistics (Historical)*, Carnegie Mellon University.(2009), at http://www.cert.org/stats/cert_stats.html#vuls.

[20] INTERNET WORLD STATS, *Usage and Population Statistics*, Miniwatts Marketing Group(2009), at http://www.internetworldstats.com/stats.htm.

confidentiality, integrity, non-repudiation, high-availability and authenticity should be deployed[21]. Thus the three basic conditions that a trusted environment must fulfil are: protected capabilities; integrity measurement; integrity reporting, all creating and ensuring platform trust[22]. Eventually systems covering these aspects will be described as trustworthy ones[23].

While the legal systems struggle to keep up with technology developments and their enforcement and prosecution, the regulation through technology took increasingly center stage[24]. Rather than prosecuting crime, the focus shifted on communicating architectures that make it impossible to commit crimes in the first place, regulating by architecture and code rather than law.

One such architecture is Trusted Computing (TC) which has been in the centre of technical, social and legal interest over the past few years, aiming to be part of our lives in the near future. TC is a new project by the Trusted Computing Group (TCG) that targets to allow the computer user to trust his own computer and for "others" to trust that specific computer[25]. In a more explanatory way, as Ross Anderson noted "TC provides a computing platform on which you cannot tamper with the application software, and where these applications can communicate securely with their authors and with each other"[26].

3. Trusted Computing Technology

The Trusted Computing Group (TCG)[27] (formerly known as the Trusted Computing Platform Alliance (TCPA)) – a non-profit organization – formed an alliance of promoters like AMD, Hewlett-Packard (HP), IBM, Intel Corporation, Microsoft, Sun Microsystems Incorporation and of contributors like Nokia, Fujitsu-Siemens Computers, Philips, Vodafone and many more and initiated the Trusted Computing (TC) project. The TCG works on the creation of a new computing platform that will provide enhanced trust to the current platform and aims to develop, define and promote standards to achieve higher security levels for the Information Technology (IT) infrastructure between multiple platforms, devices and networks[28].

TCG was formed as a result of the concerns on data exposure on systems, system compromise because of software attack and lack of methods to prevent identity theft[29]. TC is an idea which has evolved from the need to address these issues with security solutions that will mitigate the risks and dangers; and help to increase data management and identity security. Furthermore, its aim is to protect the software and data in computer platforms (servers, desktops, laptops, PDA's, mobile phones and many more)[30] from external attacks and physical theft and hopes to improve security for remote access. TC aims to add on computer hardware's functionality to "enable entities with which the computer interacts to have some level of trust in what the system is doing"[31]. This protection is provided by implementing isolated execution environments where software and data will be protected from any meddling. Trusted platforms (TP) provide such environments and define the applications that

[21] ROLF OPPLIGER & RUEDI RYTZ, *Does Trusted Computing Remedy Computer Security Problems?*, 3 IEEE Security and Privacy (2005).
[22] M. BURMESTER & J. MULHOLLAND, The advent of trusted computing: implications for digital forensics (ACM Press 2006).
[23] D. KALLATH, *Trust in trusted computing - the end of security as we know it*, 2005 Computer Fraud and Security (2005). SHIREY.
[24] LAWRENCE LESSIG, *The Zones of Cyberspace*, 48 Stanford Law Review (1996).
[25] LOHMANN VON F., Meditations on Trusted Computing (2003).
[26] ROSS ANDERSON, *Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003) at* http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.
[27] From 1999 until 2003 TCPA released a number of specifications which mainly focused in enhancing trust and security in computing platforms. In early 2001 the first specifications were released, defining the Trusted Platform Module (TPM) as the fundamental component of a trusted platform.
[28] BERGER. TCG, *Trusted Computing Group*. Trusted Computing Group (2010), at http://www.trustedcomputinggroup.org/.
[29] BERGER.
[30] G. PROUDLER, *Concepts of trusted computing*, *in* Trusted Computing (C.J. Mitchell ed. 2005).
[31] CHRIS J. MITCHELL, *What is Trusted Computing?*, see id. at (Chris J. Mitchell ed. 2008).

will be permitted to operate on selected data[32]. Additionally, TPs can offer assurances about their behaviour both in hardware and software[33]. Here we can indicate for the first time the structural similarity between TC and TM: TMs offer assurances to a human consumer that the website he is visiting abides by certain predefined minimal standards of security, TC offers assurance to a computer that the system it is going to interact with, performs to certain predefined standards of security.

The TCG project is pursuing to allow the computer user to trust his own computer and for "others" to trust that specific computer[34].

4. The analogy between TC and TMs - Learning from each other

"TMs are seen as information on somebody or something to be relied upon by others"[35]. In fact, the e-consumer is motivated from the mark (TM) on the e-merchant's website to trust that e-merchant and engage in business with him. In the case that the collaboration between the e-merchant and the TMOs doesn't work, the TM system has been proved to be weak: there were cases reported where e-consumers' personal identifying data were kept, shared or sold by "certified"-merchants without the data subject's consent and without the TMO's knowing[36].

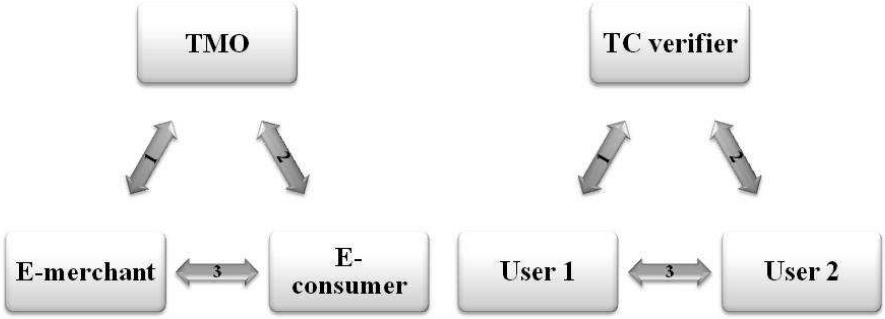
We can distinguish cases where a TM was fraudulently obtained and the TM provider did not sufficiently scrutinise the information provided in the application, situations where a certificate was once correctly issued, but the e-business subsequently lowered its standards and kept the mark on its website even after the violation was discovered[37], and situations where a website claims to have a TM it was never entitled to. All these can cause damage[38] to e-consumers[39]. Thus, it is obvious that the reliance to the trust provided by TMs can be treacherous and TMO's services require a regulatory environment to ensure reliability and accountability[40].

In our present study, we aim to provide a comparison between TMOs, and TC in order for both technologies to profit from each other. We chose the aforementioned technologies as they lend themselves for obvious analogies (see Figure 1) in the sense that TC can provide information (assurances) that a platform is to be trusted, so that a third party (i.e. another user's machine) can rely upon and proceed with successful communication and exchange of information. The user of the platform communicates with a verifier who wants to assure that the user uses the platform containing the specified TPM. In the same way TMs are seen as information that somebody or someone can rely upon by third-parties (e-consumers).

[32] G. PROUDLER, *Concepts of trusted computing*, see id. at (C.J. Mitchell ed. 2005).
[33] EIMEAR GALLERY, Who are the TCG and what are the Trusted Computing concepts? (2008).
[34] Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. (2002).
[35] BALBONI.
[36] A. MICHAEL FROOMKIN, *The Death of Privacy?*, 52 Stanford Law Review (2000);J. KORNBLUM, *FTC, GeoCities Settle on Privacy*, CNET News.com 1998. J. MCCARTHY, *TRUSTe Decides Its Own Fate Today*, Slashdot 1999.
[37] MCCARTHY.
[38] Damages include violation of e-consumer's privacy and data protection right to pure economic loss.
[39] COUNCIL EUROPEAN PARLIAMENT, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).
[40] BALBONI,

JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 3 (2012)

Figure 1: Analogy between TMOs and TC



The whole TC procedure is automated using one out of the four main features of TC technology, the *remote attestation*. This aims to allow "unauthorized" changes to software to be detected. It remotely traces any changes made to any application and allows a third party to decide whether the platform is considered trustworthy[41]. This feature helps to prevent the sending of data to or from a compromised or untrustworthy computer and certifies that no unauthorised program installs, updates or modifications are made in the hardware or software on the user's machine. Moreover, "this allows an entity to authenticate the software configuration of a platform that is not under its control"[42]. Here we can see one main difference between TC and TM: If functioning correctly, it is nearly impossible to fool the trusted third party that attests the correct working of a platform. This security comes at a "cost": the assurance provider has real time access to the computer whose safe functioning it attests, raising concerns about privacy in particular.

We can see more clearly the differences if we compare this approach with SysTrust, a TM approach initiated by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). SysTrust, is a service which aims to independently assure business and customers that an organisation's systems are reliable[43]. SysTrust procedures, in conformity with attestation standards of the AICPA, determine the effectiveness of controls that make a system operate reliably. Reliability is determined through four criteria: security (from physical or electronic unauthorized access), availability (operational readiness and access as agreed), integrity (the system should be complete, accurate, prompt, and authorized in processing of information) and confidentiality in terms of information that are kept[44].

It has been argued that such TM systems, are more marketing based than quality based, which leads to questions on the credibility of the TM system in the long run[45]. The TM provider has no incentives to probe too deeply the credentials of the company it certifies – who might desert him for a less stringent TM provider. Nor will it be always feasible to check the submitted data for its correctness – as seen above, the type of features that TM attests are much less demanding than the very formal properties assured and certified by TC. Nonetheless, the danger of opportunistic behaviour by e-traders, along with unregulated market forces, are forcing TMOs to a more untrustworthy practice[46] that needs to be altered.

[41] J. REID, GONZALEZ NIETO, J., DAWSON, E., OKAMOTO, E., Privacy and Trusted Computing § 1529 (IEEE 2003).
[42] Id.
[43] Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®) pt. 155 (2006).
[44] ENDESHAW.
[45] J. RIEGELSBERGER & M.A. SASSE, *Trust me, I'm a .com. The Problem of Reassuring Shoppers in Electronic Retail Environments*, 28 Intermedia (2000).
[46] BALBONI.

The critical questions that arise are:

1. *what e-consumers can do in order to recover the damage from their reliance on the TM* and
2. the fundamental liability question is *whether the TMOs are to be held liable to e-consumers, for their damages.*

The legal relationship between the two parties (i.e. the TMOs and the e-merchants) of the TM procedure is contractual; however, an implied tortious relationship between the TMOs and e-consumers appears as the e-consumers relied on the certificates that the TMO's issued (Figure 1). This contractual relationship cannot be excluded *a priori*.

The issue of liability of TMOs hasn't been given the appropriate attention from courts or governments, but there is a beginning of an academic debate on that issue. We argue that the same applies with the issue of liability of TC, which although it has been highly controversial amongst the scientific, academic, and legal communities, it has not been given the awareness that it deserves and in terms of academic scrutiny is even less reflective on the legal implications than the debate on TMOs[47].

As stated earlier in this paper, in cases where the e-consumer suffers damages due to his reliance on the TM that has been issued on the e-merchant's website, the consumer can sue the e-merchant for breach of contract or in tort for wilful act or breach of their duty of care (negligence liability). However, the easiness with which anyone can set up a commercial website selling products or services through the Internet[48], decreases the chance for an e-consumer to seek vindication against negligent or malicious e-merchants. Therefore, it is easier for the e-consumer to locate and sue the TMO for the provision of inaccurate information (TMs) on the e-merchants website and also request for compensation. There are TMs that use a redress mechanism that "may also have character as a third-party guarantee, where the consumer may seek redress"[49]. We argue that this integrated arbitration that TMs provide, should be adopted by TC.

Balboni[50] claims that the TMO third-party legal liability systems are inadequate in Europe and compares TMOs with Certification Service providers (CSPs) (i.e. auditors/ accountants and surveyors) which are considered TMO's equivalents, in terms of liability rules and how these apply in analogous cases. Article 6 of the Electronic Signatures Directive[51] describes third-party liability of CSPs and in England this is incorporated into the Electronic Signatures Directive in Section 4[52]. The issue of TMOs third-party liability has been at least discussed by Balboni[53] and others[54] who have analysed liability more closely and made proposal for a model of adequate TMO liability[55]. Their outcomes are described in the following section and with our present study we argue that this could be an example of how to deal with the issue of TC's reliance liability.

---

[47] YIANNA DANIDOU & BURKHARD SCHAFER, *In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security, in* Emerging Challenges for Security, Privacy and Trust (Dimitris Gritzalis & Javier Lopez eds., 2009).
[48] For an analysis on the barriers for spotting an e-merchant who has set up a commercial website see BALBONI.
[49] TRZASKOWSKI.
[50] BALBONI.
[51] PAOLO BALBONI, *Liability of Certification Service Providers Towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication*, 13 Information & Communications Technology Law (2004);EUROPEAN PARLIAMENT, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures § 43 (Luxembourg, Office for Official Publications of the EEC 2000).
[52] THE ELECTRONIC SIGNATURES REGULATIONS 2002, The Electronic Signatures Regulations 2002 (The Stationery Office Limited 2002).
[53] BALBONI.
[54] ASSAFA ENDESHAW, *The Legal Significance of Trustmarks*, 10 see id. at (2001). N. P. TERRY, *Rating the "Raters": Legal Exposure of Trustmark Authorities in the Context of Consumer Health Informatics*, 2 Journal of Medical Internet Research (2000);PETER T. WENDEL, *The Evolution of the Law of Trustee's Powers and Third Party Liability for Participating in a Breach of Trust: An Economic Analysis*, 35 Seton Hall L. Rev. 971(2004-2005).
[55] P. BALBONI, *Model for an adequate liability system for Trustmark Organisations*, 1 International Journal of Liability and Scientific Enquiry (2008).

5. The issue of TMOs third-party liability in analogy to TC reliance liability

There is almost no literature on the liability of TMOs that offers direct protection against damages caused by reliance on information[56]. As pointed out by Balboni there seems to be enough ground for improvement in the TMOs third-party liability legal issue towards e-consumers[57]. Civil liability offers protection against damages caused by reliance on inaccurate information. As there is no specific regulation covering the TMO third-party liability issue, the general principles of civil liability, tort and contract law will be applied.

The issue that arises now is that TMOs usually tend to include specific clauses[58] on their contracts in order to limit or exclude in some cases, the liability towards e-merchants and e-consumers. And this is where we see a paradox: "TMOs are seen as professionals who provide information on their clients, or their clients' practice, to be relied upon by third parties"[59] and therefore enhance e-consumer's trust. It is then highly unlikely that an e-consumer will trust e-merchant's security, privacy and business practices if the TMO - that certifies the aforementioned - refuses (through those disclaimers) any kind of liability in relation to the certificates.

From this angle, it seems like e-consumers cannot take measures to hold -TMOs liable. In fact, the chances that e-consumers have to hold TMOs liable for are very narrow under US and English law[60]. E-consumers will have to invoke either the general principles of tort and contract law or on statutory provisions and case law that may be applied in analogy to TMOs. Based on an extensive analysis done by Balboni on US and European legal systems concerning third-party liability, most commonly e-consumers will have to provide evidence

a) for the damages they incurred,

b) against the decision of the TMO to issue the TM (i.e. prove that the TMO owes a duty of care towards the consumer and that the TMO acted in a way that breached the duty of care) and

c) for the causal link between the TMO's professional fault and the plaintiff's occurred damage.

For the last point, it is a prerequisite to prove both 'foreseeability'[61] and 'proximity'[62]. However in the absence of specific provisions, third-party TMO liability will be based on policy arguments[63]. It worth to be noted that under the 2005 Directive on Unfair Commercial Practices[64], TMs can be considered as unfair commercial practice if they are not provisional on setting higher standards of consumer protection compared to the protection offered by legislation. In fact, it will be a requirement to consider advertising and user of a TM with equal levels of consumer protection and legislative requirements, as unfair

[56] MAURICE SCHELLEKENS & CORIEN PRINS, *Unreliable information on the internet: a challenging dilemma for the law*, 4 Journal of Information, Communication and Ethics in Society (2006).
[57] BALBONI.
[58] Clauses limiting or excluding the liability of TMOs to e-consumers can be found on the TMO's website. For a selection of the most commonly used clauses that TMOs are using to limit their liability see Ibid.
[59] BALBONI.
[60] Id.
[61] 'Foreseeability' determines if the harm caused to the plaintiff, resulting from an action by the defendant was reasonably able to be predicted. W.P. KEETON, Prosser and Keeton on Torts (West Group 5 Sub edition ed. 1984);RICHARD A. EPSTEIN, *Beyond Foreseeability: Consequential Damages in the Law of Contract*, 18 The Journal of Legal Studies (1989);GREEN LEON, *Foreseeability in Negligence Law*, 61 Columbia Law Review (1961).
[62] The function of proximity is concerned with how one party is placed in regard to the other party. DANUTA MENDELSON, *The law of torts* Deakin Law Review (1994).
[63] BALBONI.
[64] COUNCIL EUROPEAN PARLIAMENT, Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 (Official Journal of the European Union ed., 2005).

commercial practice, under national or community law[65]. In particular Annex I of the Directive comprises a list of commercial practices which are considered unfair.

Turning attention now to TC, it is surprising to see the same legal problem arising in the Trusted Computing (TC) legal field[66]. What happens if due to a malfunction, a non-trustworthy machine is certified as trustworthy, a third party engages with it and suffers as a result a loss? In cases such as this, legal systems can and often do impose liability outside the contractual nexus, and for the benefit of the third parties that suffered the harm. This type of delictual "reliance liability" has been discussed in the context of Certification Service Providers (CSPs) (surveyors, accountants, and auditors) which are the TMOs' offline counterparts and this will ensure that e-consumers receive at least the same protection online, as the traditional offline. As Balboni[67] pointed out in his research on the liability issue, it can be easier to deal with it, by applying the set of rules set by Article 6 of the Electronic Signatures Directive, which map out fault-based third party liability for CSPs, and postulate CSP's liability towards third-parties who suffer from damages as a result of their reasonable reliance on CSP certificates[68]. In this case, TMOs would be held liable to e-consumers who reasonably rely on the TM and then suffer loss from such reliance, for the information included in the TM at the time of issue, even though the TMO has not provided evidence of negligence, unless TMOs can prove not to have been negligent. Of course, these provisions can offer additional protection to e-consumers assuming that courts will consider them.

A literature survey suggests that while computer scientists seem primarily concerned with the technical feasibility of implementing TC, legal academics have tended to concentrate on content control and privacy issues[69]. Neither group appears to be overly concerned with an analysis of the implications of the imposition of legal liability for failure within such a system, or potential responsibility for wider social and legal concerns to which they may give rise. If greater legal responsibility is placed upon hardware/software providers, this may have a significant impact upon the speed and scope of system roll-out, and may leave the system vulnerable to threats from market pressures. A new look at the interaction between internet security, trusted computing and legal liability has been already proposed[70].

A model of adequate third-party liability for TMOs is elaborated based on the principles of CSPs liability developing the concept of 'adequacy'[71]. Through this concept, liability rules need to protect the e-consumer's expectations when trusting the TMOs, while at the same time, the difficulties that TMOs face because of their operation online should be considered[72]. The liability system needs to improve TMOs practice quality level in order to give TMs the ability to extend their potentials and benefits in social, economic and political levels[73]. The

[65] TRZASKOWSKI.
[66] DANIDOU & SCHAFER;YIANNA DANIDOU, Legal Implications of Trusted Computing (2006) (Master Thesis, University of Bristol).
[67] BALBONI.
[68] EUROPEAN PARLIAMENT;THE ELECTRONIC SIGNATURES REGULATIONS 2002;id.
[69] ANDERSON;REID;ROSS ANDERSON, *Cryptography and Competition Policy - Issues with 'Trusted Computing'*, *in* Economics of Information Security (2004);R. BRADGATE, *Beyond the Millennium - The Legal Issues: Sale of Goods Issues and the Millennium Bug*, 2 The Journal of Information, Law and Technology (JILT) (1999);A. J. CHANDLER, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 University of Ottawa Law and Technology Journal (2003);A. CHARLESWORTH, *DRM: the Straw to Break of Procrustean Approaches to Copyright?*, *in* Intellectual Property 2004: Articles on Crossing Borders between traditional and actual (Molengrafica Series) (F. Grosheide & J. J. Brinkhof eds., 2005);JOHN S. ERICKSON, *Fair use, DRM, and Trusted Computing*, 46 Communications of the ACM (2003);S. HILLEY, *Trusted computing - path to security or road to servitude?*, 2004 Network Security (2004);S. PEARSON, Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy § 3477 (Herrmann et al. ed., Springer-Verlag GmbH 2005);P. SAMUELSON, *DRM {and, or vs.} the Law*, 46 Communications of the ACM (2003);M. TURNER, BUDGEN, D., BRERETON, P., *Turning software into a service*, 36 Computer -- IEEE Computer Society (2003);C. WOODFORD, *Trusted Computing or Big Brother? Putting the Rights back to Digital Rights Management*, 75 U. Colo. L. Rev. (2004).
[70] DANIDOU & SCHAFER.
[71] BALBONI.
[72] BALBONI.
[73] Id.

ethical theory of Warranted Trust will protect both TMOs and e-consumers and develops the context in which their trust relationship is constructed[74], which aims to provide a legal solution to the expectations gap issue.

Similarly, we argue that based on the TMOs third-party liability, the TC reliance liability should be structured as statutory regulations that can be potentially applicable by analogy. The same concept of 'adequacy' which is defined by relating the trust relationship between TMOs and e-consumers should be applied in the trust relationship between TC and TC consumers.

Indeed, in many ways TC is the more obvious target of the reliance liability that Balboni discusses than TM. The TC philosophy takes the responsibility away from the user entirely and passes it on to the software and hardware producers. Imagine if the user wants to verify that a legitimate TMO is behind that TM. The user then clicks on a TM, and for his surprise is transferred to a spoofed website, and he realizes that the TMO is not the one that claimed to be. An automated system, just like a TC, ought to be able to prevent this from happening, and damages for the user to incur. Conversely, we argue that the technologically more ambitious TC approach can provide important insights into the user requirements for the next generation of TMs based on the TC philosophy and the remote attestation feature. As stated earlier, users cannot be trusted and to the extent that this is possible, an automated remote attestation should supplement TMOs.

However, in this new reality, *not* buying the product stops being an option, if not for legal, then practical reasons: unless seen as trustworthy by other machines, the computer will not any longer be able to communicate with them, or communicate fully. Where in the non-automatic TMO environment, it is ultimately a decision by the customer whether to trust a TM, or to engage with a site without one, in TC that choice will be more and more limited by design. With that, legal issues of intervening causality that could be seen as an obstacle to reliance liability are removed.

6. Conclusions

TMOs, unlike TC, rely ultimately on human judgment, and unless backed up by a strong regulatory regime could lead to a perception where TMOs are untrustworthy, in contrast with their initial aim, and non accountable. At the moment, Europe, as well as US, are arguably inefficient in specific statutory provisions and case law on TMO third-party liability which makes things harder – if not impossible – for e-consumers to enforce TMO third-party liability in cases they suffer damages from their reasonable reliance on TMs. Therefore, the TM system will be questioned and e-consumer's trust will be lost once more.

More generally, due to the unreliability of some TMOs practices, all players could ultimately be damaged: the reputation of the TM program damaged by a run to the bottom, e-merchants will run the risk of housing an untrustworthy TM which other e-merchants used and violated, and e-consumer's trust in e-commerce will decrease. Consequently, e-business and e-economies will be hurt and governments which remain reluctant to regulate in this matter will allow untrustworthy TMOs spreading out.

In fact, the absence of specific rules on TMO liability creates a legal 'immunity' for TMOs, which is unacceptable. As Balboni[75] proposed, floodgates arguments which are widely used to limit third-party liability, should be taken into consideration. As a solution, he proposed that TMOs could reasonably limit their liability as it happens, following the example of the CSP's liability provision set in Article 6 of the Electronic signatures directive[76] and European governments should sooner or later act on this issue before it is too late.

[74] BALBONI.
[75] Id.
[76] EUROPEAN PARLIAMENT.

This paper argues that TM can learn about the advantages of introducing a degree of automatisation, into this process, and into other inspection and TM qualifying activities, and in the general outline of an infrastructure similar to TC. Additionally, we argue that based on the TMOs third-party liability, the TC reliance liability should be structured using the same concept of 'adequacy' which is defined by relating the trust relationship between TMOs and e-consumers and should be applied in the trust relationship between TC and TC consumers. Lastly, TC is, in our view, an even better candidate for reliance liability than TMOs, as the more automation is adopted by TMOs, the stronger is their case becoming for reliance liability.

* * * * *

Cite as : Yianna Danidou & Burkhard Schafer , *Legal Environments for Digital Trust: Trustmarks, Trusted Computing and the Issue of Legal Liability*, Journal of International Commercial Law and Technology, vol.7 Issue 3 (July, 2012)